UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/060,039	01/30/2002	Edward M. Scheidt	STS 139	6541

7590 12/09/2003

IP STRATEGIES, P.C.
Suite 301
806 7th Street N.W.
Washington, DC 20001

EXAMINER	
ARANI, TAGHI T	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 12/09/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/060,039	SCHEIDT ET AL.	
	Examiner	Art Unit	
	Taghi T. Arani	2131	

-- The MAILING DATE of this communication app ars on the cover sheet with the correspondence address --

Period for R ply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE ____ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *01 October 0203*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *13-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *13-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1- Claims 1-30 were pending for Examination.

2-Claims 1-12 are cancelled.

3-Claims 13-30 are pending for examination.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 13-18 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 13 recites the limitations "restricting the user's access to the system if the user's identity is not authenticated, based at least in part on the authentication value"" in paragraph 3 and " granting the user's access .....if the user's identity is authenticated, based at least in part on the authentication value" same page, paragraph 4. There is insufficient antecedent basis for the limitation "the authentication value" in the claim.

Claims 14-18 are rejected by virtue of their dependencies.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 13-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over prior art of record, US Pat. No. 5,280, 527 directed to Gullman et al. and US Pat. No. 6,317,834 directed to Gennaro et al.

Claims 13, 17-18, 19, 23 –25, 29-30 are amended to replace the "key" wit the " first cryptography key" and to replace " an authentication value" with " a second cryptography key" By reviewing the specification, the terms "authentication value" , " validated key" and " cryptography key" are used interchangeably. Hence, for the purpose of applying art the examiner assumes that "second cryptography key" recited in claim 13 and "cryptography key" recited in claims 13, 17-18, 19, 23 –25, 29-30 can be broadly and reasonably interpreted as "authentication value", see page 15 lines 1-2, page 7, lines 1, 22, page 18 line 15, page 9 line 11-12, page 12, line 21 and page 14, line 17 of the specification.

As per claims 13-14, 19-20 and 25-26, Gallman teaches a biometric security mechanism which generates a security token which a user inputs to an access device. Gullman's security token is formed from biometric information (i.e. biometric-based data instance), a fixed code and, a time varying code, see col. 3,lines 37-55. Gullman's fixed code includes a PIN (i.e. knowledge-based data instance), embedded serial number, account number (i.e. possession-based data instance), see col. 2, lines 48-65.

Gullman further teaches that the security apparatus receives the biometric input, and then compares the biometric input to a stored template to derive a correlation factor. The correlation factor is combined with the fixed code to generate a security token (i.e. an authentication code).

Gullman further teaches that the security token is displayed on a display panel of the security apparatus where it is entered at an access code or is directly transmitted to a host system

which decodes the token to identify the embedded fixed code and correlation factor, see col. 4, lines 3-22.

Gullman teaches that the host system determines whether to grant to user the access to the host system. This determination is based on a comparison made on a transmittable code which includes the above described authentication code, see col. 7, lines 1-33.

Gullman teaches that the processor of the security apparatus may include a standard encryption module which applies an encryption algorithm to the time of day from real time clock, the fixed code (which includes PIN, serial number and account number) and a biometric correlation factor, generating an encrypted security token (that is, an encrypted authentication code). Gullman further teaches that the host system also includes a decryption module, capable of decrypting the encrypted code generated by the encryption module of biometric security apparatus, but fails to specifically disclose " generating a key based on a first data instance of the plurality of factor-based data instances" and "applying the key to at least one modified data instance to generate a recovered data instance" and " interrogating the recovered data instance against the second data instance to generate an authentication value".

However, Gennaro teaches a method of performing biometric authentication of a person's identity including a biometric template prior to storing it in a biometric database, see abstract.

Gennaro's method further provides means for verifying the identity of an individual to authorize access to a general database comprising the steps of:

Acquiring a current biometric sample (i.e. a biometric-based data instance), acquiring a current personal identifier (i.e. a knowledge based data instance); acquiring decryption key generation data (i.e. a plurality of factor –based data instances); comparing the personal

identifier with the database, and on a match with a personal identifier in the database; creating a decryption key from decryption key generation data; performing a decryption operation on the retrieved biometric (i.e. recovered biometric) record utilizing the decryption key to decrypt encrypted biometric model from the retrieved record. Comparing the decrypted biometric model with the current biometric sample to verify the individual as authorized to access the general database, see col. 2, line 6-21.see also Fig. 5 and 6.

Gennaro further teaches that a first encryption key is created from the user's password (i.e. one of factor of plurality of factor-base data instances) and is used to encrypt the biometric model. That is, a modified data instance is created based on a second data instance of a plurality of factor based data instances.

It would have been obvious to one ordinary skill in the art to modify Gullman's biometric security apparatus to employ Gennaro's method of authentication with encrypted models to store biometric information in a secure manner so as to prevent the occurrence of theft and attacks from unauthorized personnel, see also 1, lines 40-55.

As per claims 15 – 18 and 21-24, 27-30, Gullman teaches that the security apparatus initially is configured in an enroll mode where biometric samples or templates (i.e. first biometric data instance) are obtained. Gullman further teaches that the access device transmits a derived token (i.e. a second modified version of biometric data instance) to the host system, which decrypts or decodes the token to derive the fixed code and a correlation factor. If the fixed code identifies a valid user and the correlation factor is above the threshold level, then access is permitted, if not, then access is denied, see col. 6, lines 30-45.

Gullman fails to teach a modified version of biometric data instance where the modified version is a cryptographic hash of second biometric-based data instance.

However, use of hash function and message digest using a one directional hash function is well known in the art of cryptography, this is taken as official notice. It would have been obvious to one ordinary skill in the art to hash the biometric templates or samples of Gullman at enrollment for security and space requirement.

Response to Amendment

Applicant's arguments filed on 10/01.203 regarding the rejection of the claims 13-30 under 35 U.S.C. 103() have been fully considered but they are not persuasive.

As per Applicant's arguments relating to rejections of claims 13, 19 and 25, the Applicant merely argues that Gullman generates a "security token based on biometric information and either time-varying information or a user-input challenge code", page 10, third paragraph, and that Gullman's definition of security token is not a cryptography key, page 10, same paragraph. The Examiner disagrees for the following reasons.

As stated above, in view of Applicant's own definition and description of a cryptography key is "a validated key" created by binding the factors together to provide authorization", page 7, line 1-3 (of disclosure) and that " a validated key" c is used directly.... as an access code.

Applicant further describes that "the user's access to the system is granted if the user's identity is authenticated, based at least in part on the authentication value", page 9, lines 15-18. That is, the "authentication value" and the generated "cryptography key" are used interchangeably throughout the specification and the exemplary embodiments.

By broadly interpreting the "cryptography key" as an "authentication value" (page 15, lines 1-2), the examiner responds security apparatus of Gullman "receives a biometric input from a user, which then is compared to a template to determine a correlation factor. The correlation factor, a fixed code and either a time varying code or a challenge code then are combined to generate a token", emphasis added, see abstract (Gullman), and that the fixed code comprises factors (i.e. possession-based instance) such as PIN, embedded serial number, account number, see page 4, lines 3-21.

Applicant does not provide any argument regarding lack of a motive to combine the references. Applicant merely points out that the feature of combining a factor-based data instances to arrive at a cryptography key are not taught by prior art of record. This doe not constitute a proper challenge to the combination of two references.

Action is Final

THIS ACTION IS FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Conclusion

Any inquiry concerning this communication or earlier communications from examiner should be directed to Taghi Arani, whose telephone number is (703) 305-4274. The examiner can normally be reached Monday through Friday from 7:30 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (703) 305-9648. The Fax numbers for the organization where this application is assigned are:

After-final (703) 746-7238

Official (703) 746-7239

Non-Official/Draft (703) 746-7240

Taghi Arani

Patent Examiner

December 3, 203

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100